

### REMARKS

Claims 1, 3-14, 16, 17, 19, 20, 22-33, 35, 36, 38, 39, 41-52, 54, 55, and 57 are pending with claims 1, 20, and 39 being independent. Claims 2, 15, 18, 21, 34, 37, 40, 53, and 56 are cancelled by this amendment without waiver or prejudice.

Claims 1-57 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cox (U.S. Patent No. 6,738,814) in view of Maher (U.S. Patent No. 6,654,373). Applicants respectfully traverse the rejection.

Applicants have amended claim 1 by incorporating the features of claims 2 and 18. As amended, claim 1 recites a method for securing an accessible computer system that includes, among other features, scanning the payload portion of data packets for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern. Access by an access requestor to an access provider is denied when the number of payload portions that include the predetermined pattern exceed a configurable threshold number.

Applicants respectfully request reconsideration and withdrawal of the rejection because Cox and Maher, either alone or in combination, fail to disclose or suggest scanning and counting a number of data packets having payload portions that include a predetermined pattern and denying access once the number of packets having the pattern exceeds a configurable threshold number.

Rather, Cox describes blocking denial of service attacks and address spoofing attacks by identifying known patterns for these types of attacks. For instance, Cox describes identifying a denial of service attack by looking for unacknowledged data packets or identifying an address spoofing attack by looking for a source address that matches an internal address of a private network. See Cox, col. 1, line 55 to col. 2, line 8. Thus, Cox identifies these types of attacks by looking for unacknowledged data packets and source addresses that match a private network's internal address.

Cox does not describe or suggest blocking attacks by scanning and counting a number of payload portions of data packets having a predetermined pattern and denying access when the

number of payload portions that include the predetermined pattern exceed a configurable threshold number.

Furthermore, the office action does not point to any support in either Cox or Maher for the rejection of the feature recited in claim 2, which is now incorporated into amended claim 1. Specifically, the office action does not provide any support to reject the feature of counting the number of data packets having payload portions that include the predetermined pattern.

Since Cox does not describe or suggest counting the number of data packets having payload portions that include the predetermined pattern, it follows that Cox also does not describe or suggest denying access when a number of the payload portions having the pattern exceed a configurable threshold number. This feature was recited in claim 18 and is now incorporated into amended claim 1. The office action points to Cox col. 3, lines 11-29 and col. 4, lines 16-40 to support the rejection of the feature of claim 18. However, in col. 3, lines 11-29, Cox merely describes identifying a spoofed packet or an unacknowledged packet and blocking an attack when one of these attack patterns are identified. In col. 4, lines 16-40, Cox merely describes denying access if a connection to the source already exists. Nowhere does Cox disclose or suggest counting the number of payload portions having a predetermined pattern and denying access when the number of data packets having the predetermined pattern exceeds a configurable threshold number.

Maher does not remedy the failure of Cox to describe or suggest these features. Instead, Maher describes a packet analyzer that scans the contents of each data packet, classifies the data packet and processes each data packet based on its classification. See Maher, Abstract. Notably, the office action does not rely upon Maher to support the rejection of the features of claim 2 or claim 18, both of which are incorporated into amended claim 1.

For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 1 and its respective dependent claims.

Similarly to claim 1, each of independent claims 20 and 39 have been amended to recite an arrangement that includes scanning and counting the payload portions of data packets for a predetermined pattern and denying access when a number of the payload portions having the

Applicant : Brian Jacoby et al.  
Serial No. : 09/894,918  
Filed : June 29, 2001  
Page : 13 of 13

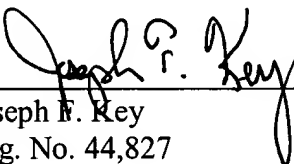
Attorney's Docket No.: 06975-203001 / Security 14

predetermined pattern exceeds a configurable threshold number. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 20 and 39 and their respective dependent claims, for at least the reasons discussed above with respect to claim 1.

No fees are believed to be due. However, during the pendency and the prosecution of this application, please apply any deficiencies or credits to deposit account 06-1050.

Respectfully submitted,

Date: 3/7/2005

  
\_\_\_\_\_  
Joseph F. Key  
Reg. No. 44,827

Fish & Richardson P.C.  
1425 K Street, N.W.  
11th Floor  
Washington, DC 20005-3500  
Telephone: (202) 783-5070  
Facsimile: (202) 783-2331